

Information security - IV
Prof. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module - 26
Lecture - 26
Client Side Attacks Tools in Kali Linux

So, in this session we are going to continue our discussions on the cracking tools that are typically used for cracking the password. So, we had a very very brief look at how was generally the approach that is actually taken for tracking the passwords. And then we also had a very brief look at depending on the operating system of whether it is windows on whether it is Linux; what kind of mechanisms are generally followed for cracking the passwords in the previous session.

In the session, we going to take a look at few tools that are actually available including a demo of one of the tools. So, that we get more familiarity on how to use those tools and try to see if the passwords could be cracked.

(Refer Slide Time: 00:56)


[Kali Linux: Johnny?](#)

Johnny is a GUI for the very popular John the Ripper password cracking tool.

Johnny has several engines that allows it to crack different types of passwords, including encrypted and hashed passwords.

Can auto-detect most hashes and encrypted passwords, making the process easier for Penetration Testers. Very easily customizable and can be configured in different ways to speedup password cracking.

Available in Password Attacks | Offline Attacks and select Johnny. Click on Open Password File and select the password file you want to crack.



There was actually a tool that we talked about involving the server side attack where we looked at the John the Ripper crack password cracking tool. So, we have a GUI version of that tool called as Johnny that is actually available in Kali Linux. This is actually a GUI wrapper on top of the CLI tool; the John the Ripper CLI tool, which actually has the

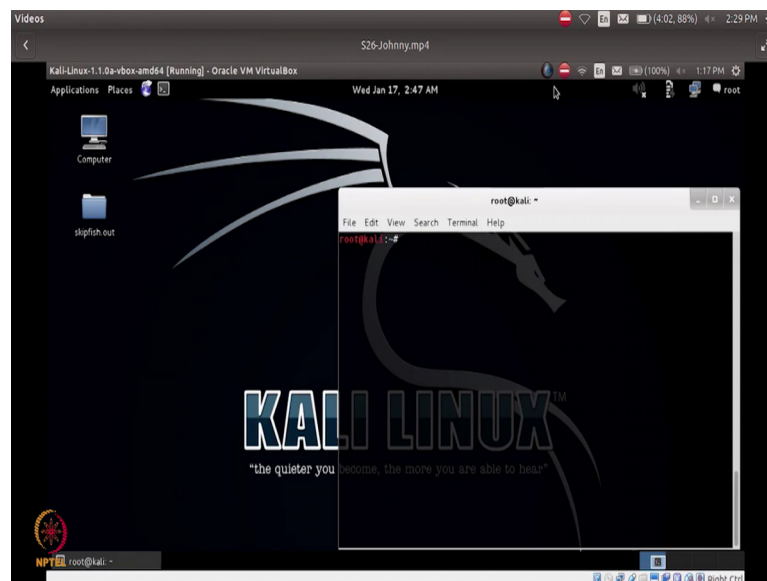
several engines that basically tries to crack the different types of passwords that could potentially be used right ah; so, in the given file.

So, the beauty of this tool is that it can do auto detect most hashes in encrypted passwords; making this as a one of the most favorite tools that is typically used by penetration tester. So, depending on the different types of hashing algorithms my target could actually be using. So, like we were discussing earlier; so, now, different types of hashing algorithms like MD 5, SHA and so, on and so forth.

This tool has a mechanism to auto detect the hash that is actually used on the given password file. And then try to apply the hashing algorithm based on either a word list or a dictionary or whatever options is actually been set on that two right top. So, this is something which is actually available in the password attacks menu option of Kali Linux under that it is available in the submenu of offline attacks.

So, once you go to offline attacks you select Johnny and open up the tool right.

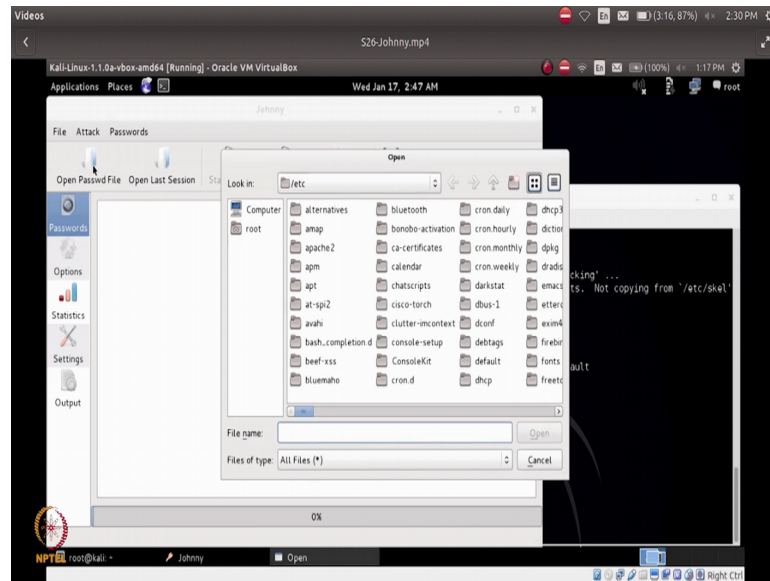
(Refer Slide Time: 02:26)



So, we will actually see a small demo of how this tool is actually working. So, while we look at the demo what we will really tried to do is we will first try to add a user which will typically have a very very small password which could potentially be very easily hacked by other penetration tester right.

So, we are just having a small password set for this user while creating the user and then we are now going to start the Johnny a tool under on offline attacks. So, it now opens up a GUI for me where I could actually say I want to open up a password file and I want to open up a last session, whatever the last session was actually doing right or I could specify the different type of options that I want to have and. so on.

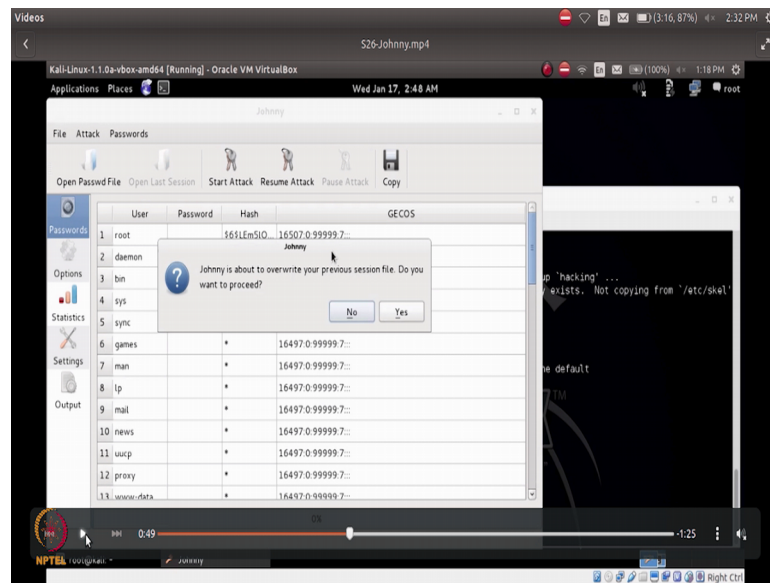
(Refer Slide Time: 03:20)



So, we will now take a look at few of those things; so first we are going to specify the password file that we want to open. And so, the password file that you are going to decide is to use the etc shadow file. So in the etc directory; so, we are going to basically make use of the shadow file which is basically the file in which I am going to have my hashes stored.

Now that we are actually created a user called hacking in that particular system on which you are running the tool. So, the hash hash signature for this particular password will also be available as part of my etc shadow file right.

(Refer Slide Time: 03:57)

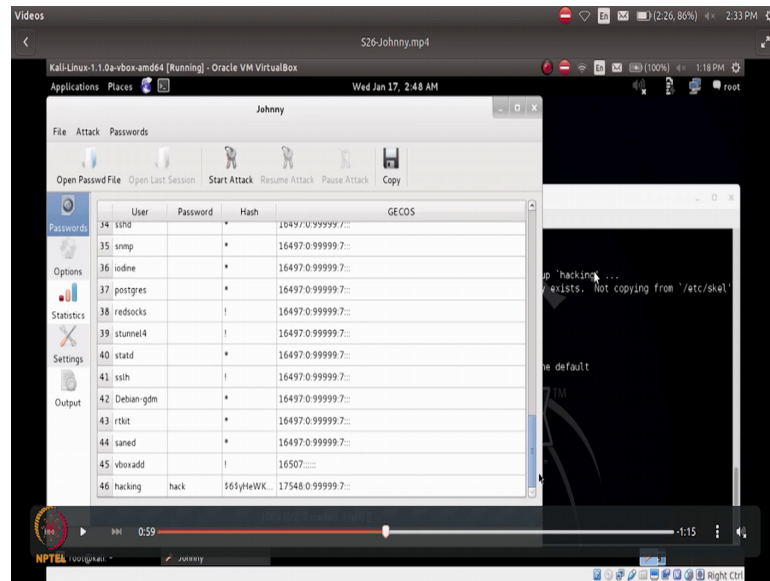


So, if you look at this right now it is basically once we say the after saying the password file, if you do a start attack it basically gives as a warning saying that the previous session file that was actually ran after the tool has been opened up has not been saved right. So, do we want to basically go ahead proceed and then overwrite this session right.

So, it basically gives you this warning; so, that by mistake or by accident we do not sort of overwrite the existing session if we had not gone ahead and saved the previous sessions output. So, if you actually over right this option and then still ask it to go ahead and proceed, it basically list down the two passwords that it is actually cracked.

So, if you see here the first one the root; by default as we already know by now the default password for the root user on a Kali Linux is toor that is a reverse of root so, it has now successfully given this string and also displayed the hash value right.

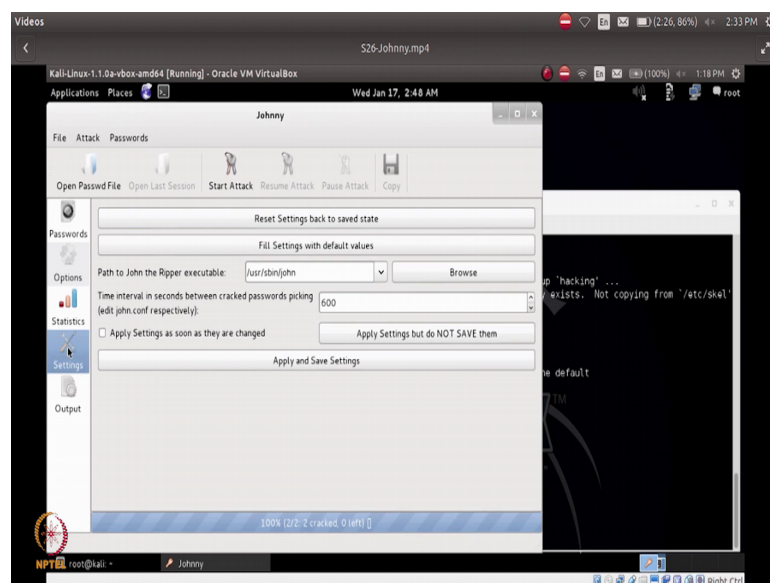
(Refer Slide Time: 05:05)



Now, similarly it is also will tell you that the last created user hacking that we actually created in this session before we started the tool; it has also cracked that password and the password it is reporting correctly has hacked along with the hash value that it is actually generated and tested successfully for this particular string right.

So, likewise it will basically go ahead and tell you the passwords for different users that is actually available in the shadow file.

(Refer Slide Time: 05:36)

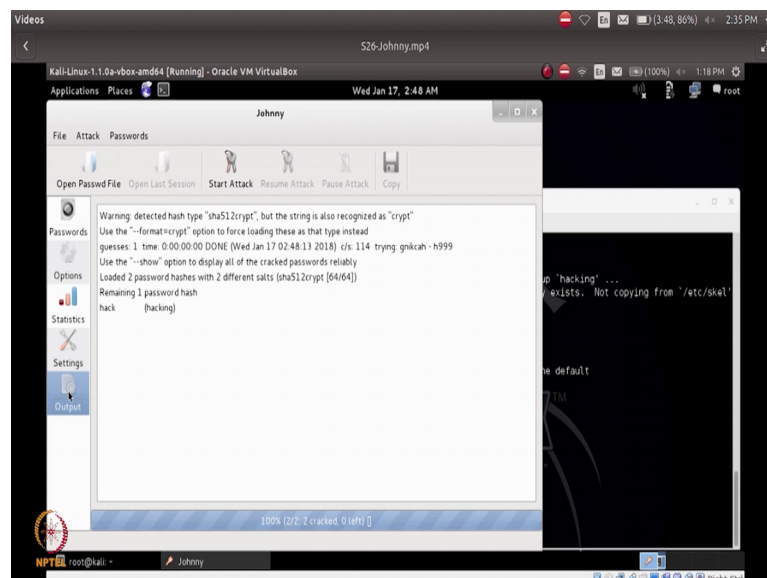


So, if at all I actually have a password which is very long or which is a combination of characters alpha; alpha numeric characters, punctuation symbols and so, on ah; you will find that the time that this tool is actually taking you will be much much more and then it will actually show you the status bar at the bottom of the tool; where in it will say like you are seeing the screen right now ah.

It will say how many passwords, how many hash values it has a potentially got from the shadow file and out of which how much it is actually trying to retrieve now right. So, that will basically give an indication saying that it has been able to complete all the cracking of all the password, but it could potentially do or how much of it is still remaining to be done right.

So, like for example, in this screenshot now it basically says that it is 2 out of 2; that means, it has been able to detect 2 hash values and it has been able to successfully crack both those hash values and then report it to us right. So, in the settings button you have a different type of settings that you could potentially do if you want to change any of those settings and then save the settings; so, that it is actually available every time you open up this tool for use.

(Refer Slide Time: 06:55)

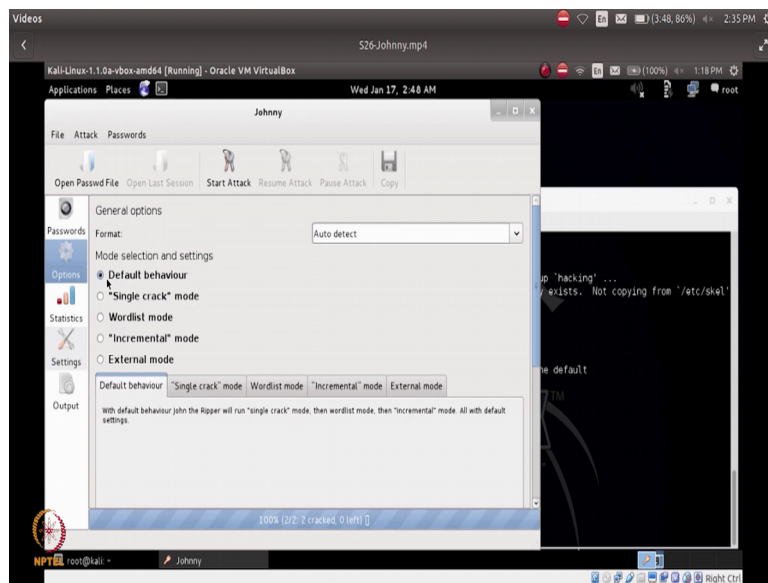


So, the output screen will actually be reporting you the output that you generally get in the command line. So, if you remember this is the typical output that we actually saw as

part of running the tool John that is a CLI version of this tool in the command line in in few of in the in few of the sessions are before our current session right.

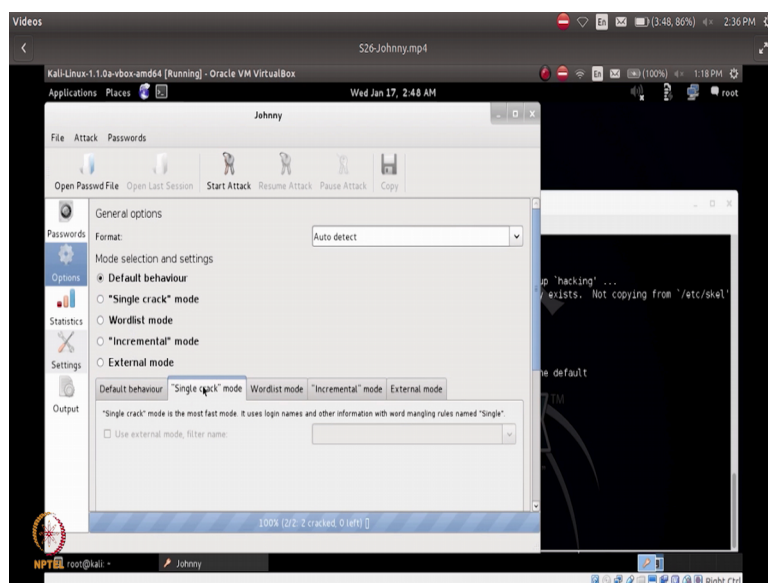
So, it is basically telling you that it has actually been able to generate one password hash successfully till now right. So, it is basically telling you the output that you will generally get as part of the command line version of this.

(Refer Slide Time: 07:30)



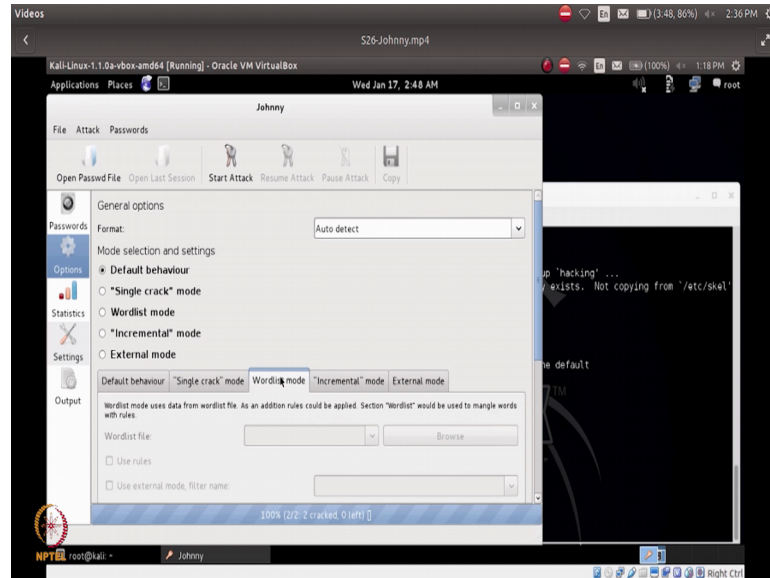
And then in the options it will basically list you the various options that is there. So, it could be either the default behavior single crack wordlist or incremental or external right.

(Refer Slide Time: 07:40)



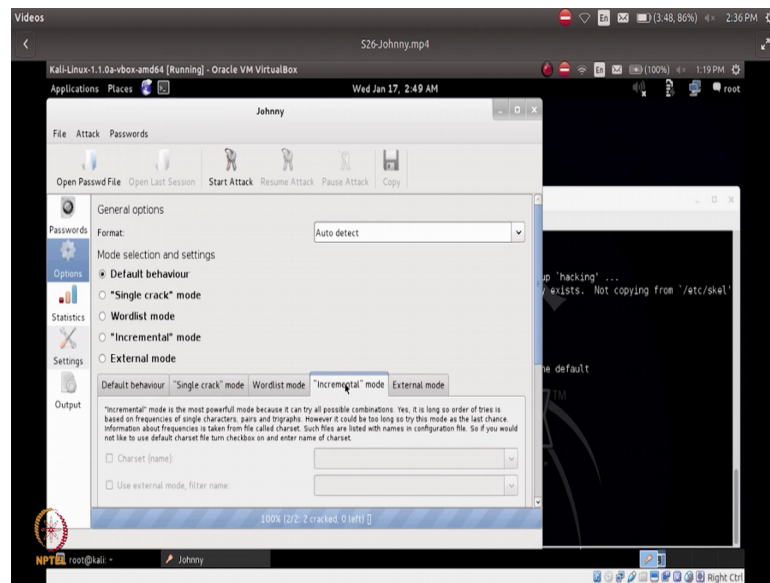
So, the single crack method basically means it is basically the most fastest mode that is used and it basically uses very commonly you known login names and passwords.

(Refer Slide Time: 07:55)



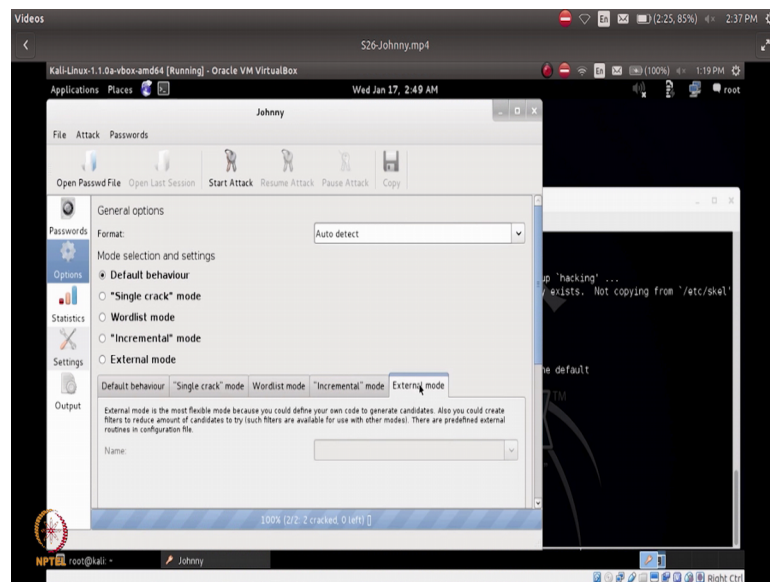
Now, in the word list what I could actually specify what is a wordlist file that it has to take as an input and compare. And you will send find that all these are actually grade out right now because the word list mode is not enabled here has the option. So, if I enable the word list mode; you will find that these are enabled for you to appropriately give inputs for this particular selection right; so similarly incremental mode and then the external mode right.

(Refer Slide Time: 08:20)



So, in the incremental mode it will basically try to have all kinds of combinations possible which you could actually test it out maybe a single; single crack mode combined to the word list mode and so, on and so, forth right.

(Refer Slide Time: 08:34)



So, external mode is basically you have your own code to basically generate the different kind of a strings with which it has to be tested or done the brute force attack with and thereby you will actually be able to do the penetration testing of cracking the passwords very effectively.

(Refer Slide Time: 08:55)

[Kali Linux: hashcat?](#)


hashcat and oclHashcat are password cracker utilities.

These are multithread tools that can handle multiple hashes and password lists during a single attack session. Offers many attack options: brute-force, combinator, dictionary, hybrid, mask, and rule-based attacks.

Available in Password Attacks → Offline Attacks

To use hashcat on a document, type hashcat [options] hashfile [wordfiles]directories . The following example shows hashcat running a wordlist against a shadow file:

```
root@kali:~# hashcat /root/Desktop/shadow /root/Desktop/wordlist.lst
initializing hashcat v6.44 by atom with 8 threads and 32mb segment-size...
```



The next tool that is actually used is what is called as a hashcat tool. So, hashcat and ocl hashcat are basically again password cracker utilities that are available. So, one main difference in this tool is these are actually multi thread tools that could potentially handle multiple hashes and passwords lists in a single attack session right.

So, if you are target on which you are running these tools are a little bit more powerful and also could leverage the multiple course that are possible there on that particular target mission ah; then this tool will be more powerful in the sense that it could actually run at a much faster place and then generate and give you the final output more quickly right.

So, this is basically the soul major difference or I would say the most important difference in this tool with which the same data points could be actually run in a much more faster manner. Because you could potentially have multiple threads running at the same time with this tool and each thread could actually handle hash or and a password list for looking at it as a single attack session right. So, this again the tool is actually available under the off line attack submenu of the password attacks in the Kali Linux menu option.

And the way to actually use this tool in the command line will be like saying hashcat followed by the hash file and followed by the word list file that has actually been that is required to be used as a parameter for running this cracker program right. So, for the


windows you actually have a tool called samdump 2 that is again available in offline attacks.

(Refer Slide Time: 10:34)

[Kali Linux: samdump2?](#)
Utility that dumps the Microsoft Windows password hashes from a SAM file so that they can be cracked by an offline tool. For newer versions of Windows, you will need another tool to capture the SYSKEY (boot key) file to access the hashes stored in the SAM database.

samdump2 can be found under "Offline Attacks". When you open samdump , a Terminal window will pop up.

You must mount your target Windows system so that samdump can access the SAM file.
Next, copy the SAM and SYSTEM files into your attack directory.
cp SAM SYSTEM /root/AttackDirectory



So, for the newer versions of this newer versions of windows as we were discussing before you need another SYSKEY called as a boot key that is also required to access the that SAM database right.

So, if one accesses the target windows system by booting this system in a different ways and then mountain mounting the windows system as NTFS partition or NTFS file system on the Linux OS for example, then they could actually try to have the SAM and the system files copied into a separate directory called root attack directory on which I will basically have the samdump 2 command a utility run right.

(Refer Slide Time: 11:23)

Kali Linux: samdump2?

Navigate to the attack directory and issue bkhive SYSTEM bootkey to obtain the bootkey. Copy the bootkey into a text file so that samdump has the SAM file with bootkey

```
cd /root/AttackDirectory > windowshashfiles.txt
```

Execute samdump using the samdump SAM bootkey command. Copy the output into a second text file.

```
Samdump2 SAM bootkey > windowshashfiles2.txt
```

Now use a password cracking tool such as John the Ripper to crack the hashes!



This is basically a what is a tool that is actually available for trying to generate the the hash files ah; I mean the hash strings and the output could actually be generated into the single hash file right. So, now, this hash file which is basically the output file generated out of running the samdump 2 command could actually be given as an input now to my tool like a John the Ripper.

Because as we have been seeing the CLI and the GUI version of the John tool ah; it basically requires only the hash file. So, as long as it has got a hash file with the hash strings in it, it is basically going to run and try to find out how it can effectively crack with the word list file or the dictionary or whatever it is and try to generate the password associated for that right. So, in that way we could also be successful in generating the cracked passwords for a windows system.


(Refer Slide Time: 12:35)

[Kali Linux: chntpw?](#)

chntpw is a tool that resets local passwords on Windows 8 and earlier versions of Windows. It modifies the Windows password database. This tool is primarily used for getting into Windows boxes when you do not know the password.

To use chntpw, boot up the Windows machine with the Kali Live CD.

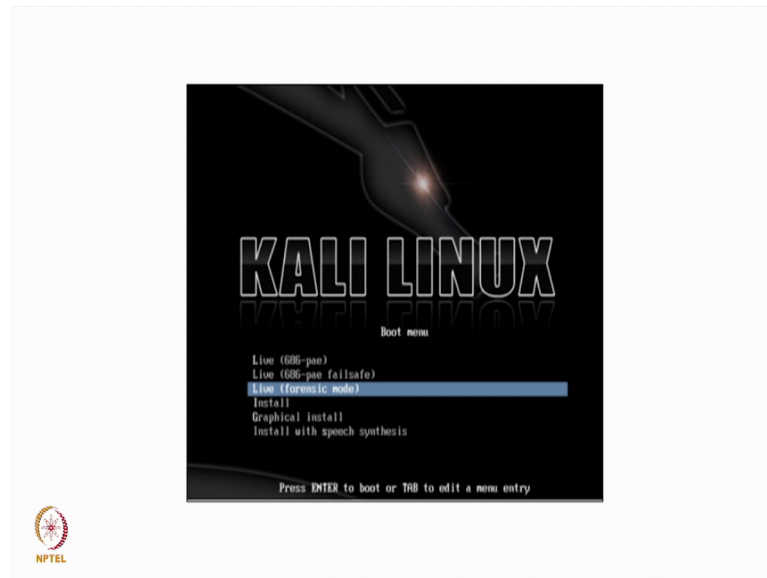
On the boot menu for Kali, select Forensics option.



So, another tool that is actually available on windows a specifically is what is called is chntpw. So, this is something this is the tool that is typically used for resetting the local passwords on any kind of an operating system from Windows 8 right. So, up to Windows 8 or even earlier versions of Windows, you could actually run this tool and then try to successfully reset the password of the Windows OS right.

So, ; so if at all I basically have windows system in which I do not know the password for getting into the windows system ah; this tool could potentially come in handy at that point in time. Now for running this tool I will need to actually boot up the other machine; Windows machine with the live CD of Kali Linux available; so, it needs to have a CD drive preferably in which I put the Kali live CD.

(Refer Slide Time: 13:41)



And then try to boot the that particular system and then select the forensics option that actually comes with the live CD right. So, that is basically the OS that we will actually try to sort of use at the time of booting it up.

(Refer Slide Time: 13:53)

[Kali Linux: chntpw?](#)

The SAM file is usually located under `/Windows/System32/config` .

The SAM database is usually in the `/media/name_of_hard_drive/Windows/Svstem32/confia`.

```
root@kali:~/media/EC08E2D208E29ABA/Windows/System32/config# pwd
/media/EC08E2D208E29ABA/Windows/System32/config
root@kali:~/media/EC08E2D208E29ABA/Windows/System32/config#
```

The command `chntpw -l SAM` will list out all the usernames that are contained on the Windows system.

```
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length
Password history count
RID | Username | Admin? | Lock? |
---|---|---|---|
01f4 | Administrator | ADMIN | dis/lock |
03e8 | alakhani | ADMIN | |
01f5 | Guest | | dis/lock |
03ea | HomeGroupUser$ | | |
root@kali:~/media/EC08E2D208E29ABA/Windows/System32/config#
```

An NPTEL logo is visible in the bottom left corner of the slide.

And then go into the forensic mode of the Kali Linux, where I will actually have the SAM file located under the windows system 32 config.

So, windows system 32 system; 32 here is expected to be your system partition of your windows OS as. So, under that I will basically have the config file and whatever is the

drive that in which I actually have this; you I you I will basically try to have that accessed under slash media slash name of hard drive. So, if it is basically for example, is htv 1 right; so, I will actually have media hdv 1 or some time some system basically gives us some number here which is basically an idea that is generated.

So, whatever it is the name of the hard drive in this command in this particular path has to be changed appropriately as mentioned as applicable for that particular system. So, in this particular case if you see it is basically a string that is actually generated. The SAM data base will basically be available to you to be available in this particular mounted location right.

So, on that if we run the command chntpw minus l SAM, it will list out all the usernames that are basically contained on the windows system. So, the output does be something like this right; so, what is the different username that are actually available right.

(Refer Slide Time: 15:11)


Kali Linux: chntpw?
chntpw -u "Administrator" SAM, and we got the following menu:

```

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account (seems unlocked already)
q - Quit editing user, back to user select
Select: [q] >

```

We now have the option of clearing the password, changing the password, or promoting the user to administrator. Recommendation is to clear the password. By doing this, you will be able to log into the target system with a blank password.



So, if you are basically use then chntpw minus u Administrator SAM; we get the following menu where in it basically list down the output in this manner. And if you find that there is an option specifically for clearing the password, changing the password and or trying to change the privileges of a particular user to that of an Administrator rights.

So, our recommendation would be to actually go ahead and just clear the password here after which you can reboot that particular system and then login into the system as an

administrator by using the changed password through the which you are done as part of the chntpw command this particular command right.

So, with this tool if at all we are we are basically locked up with the windows system for which we do not remember the password or the password modification at actually got corrupted or whatever it is ah; we could actually go ahead and try to make use of this utility where in you could actually reset the password of the administrator for example. And then once you are successfully reset the password, you could go ahead and try to reboot the system of with to the windows operating system and login into that system successfully. So, this is that this is a utility that will come in handy; whenever we have a requirement to reset the password.

Thank you.